LAUREA
AMMATTIKORKEAKOULU
Uuden edellä

Information Security in Smart Electricity Metering

Siiteri Lauri

2013 Leppävaara

Laurea University of Applied Sciences
Laurea Leppävaara

Information security in smart electricity metering

Siiteri, Lauri
Tietojenkäsittelyn koulutusohjelma
Bachelors degree of Business information Technology
November 2013

Laurea-ammattkorkeakoulu
Laurea Leppävaara

Tiivistelmä

Siiteri, Lauri

Etäluettavien sähkömittareiden tietoturva

Vuosi 2013 Sivumäärä 31

Suomen valtio haluaa, että kuluvan vuoden loppuun mennessä 80 prosenttia ihmisten sähkömittareista on etäluettavia. Vaikka lähes kaikki Suomessa toimivat sähköyritykset ovat asentaneet vaadittavan määrän mittareita, muunlaisia asioita on jäänyt auki. Asennusprojektin ollessa jo näin pitkällä on noussut kysymyksiä muun muassa siitä, kuinka todennäköistä on mittareiden välittämän tiedon hyväksikäyttö ja kuka siitä voi hyötyä.

Tässä tutkimuksessa selvitän mittareiden tietoturvallisuutta asiakkaanani toimivalle, etälukupalveluita kotimaiselle sähköntuottajalle tarjoavalle yritykselle. Käyn läpi myös sen, kuinka suurta vahinkoa voidaan tuottaa, mikäli mittaripalveluita tuottavan yrityksen järjestelmiin kyetään murtautumaan. Tämän pohjalta kyseinen yritys tulee parantamaan omia järjestelmiään ja käytäntöjään mahdollistaakseen mahdollisimman suojatun järjestelmän. Koska tutkimus tarkastelee aukkoja asiakasyrityksen tietoturvassa, kaikkia yksityiskohtia ei voida tuoda julkisesti esille. En myöskään tuo julki asiakkaanani toimivan yrityksen nimeä. Tutkimus ei koske pelkästään mittareilla olevaa tietoa vaan kaikkia pisteitä mittarilta sähköntuottajan järjestelmiin.

Tutkimuksen aikana kohtasin joitain vaikeuksia. Vaikka etäluettavat mittarit ovat yleistyneet maailmanlaajuisesti ja niitä koskevaa tutkimustietoa löytyy kohtalaisen paljon, niistä tehtyjen tietoturvatutkimusten saaminen on erittäin vaikeaa.

Tutkimusta tehdessä on käytetty hyväksi kahden kahden asiantuntijan haastatteluja, tutkimuksia mittareiden tietoturvasta sekä kansainvälisen median internetissä julkaisemia uutisia mittareista ja niiden tietoturvasta.

Asiasanat: Tietoturva, sähkömittaus, tietojärjestelmät

Laurea University of Applied Sciences
Laurea Leppävaara

Abstract

Siiteri, Lauri

Information Security in Smart Electricity Metering

Year 2013 Pages 31

According to the strategy of the Finnish Government, before the end of the year 2013 at least 80 per cent of electricity metering should be made by meters capable of remote reading, so called smart meters. As most of the Finnish electricity utilities have installed the needed number of meters, some other issues have been left open. When the installing process is almost over, questions have arisen about the likelihood of someone trying to gain advantage of the information the meters hold and who might be able to use that information.

This research examines the security issues of smart metering for the client company, sellers of remote reading services for one Finnish electricity utility. The study will also focus on how large devastation it might cause if someone is able to break in to the systems of the metering service provider. This research will be used by the company to make their processes and systems more secured and to ensure a metering system as secured as possible. Because this research concerns information security and there are also holes in the systems, there will be some classified data left out of it. For the same reason the company name will not be mentioned. The research does not only concentrate on the meter level; it will also monitor every step of the data from the meter to the utilities systems.

During the research project a few problems occurred. Even though the smart meters have become common and there are plenty of researches about them, it is difficult to find research on their security.

Interviews with two smart metering experts as well as researches and news in the international press have been utilized as background data while working on this thesis project.

Keywords: Information security, smart metering systems

Table of Contents

1 Introduction

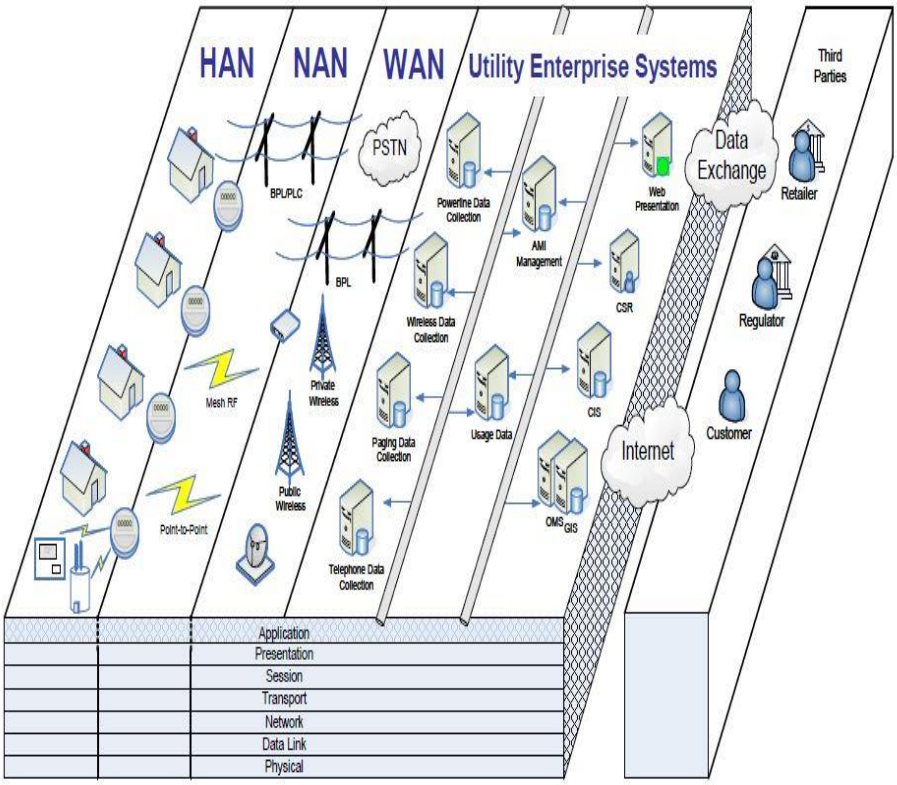

Figure 1: Figure: Picture above presents the smart metering architecture. From there we can see all the layers which must be secured to keep the meters, the data and the utilities network safe.

I decided to help my current employer by doing my thesis about security issues in smart metering. I will go step by step from a meter to the Electricity Company and figure out possible security issues and risks and identify them. I will also advance how to minimize the risks. I will take a look at smart metering processes as a whole, so I will not concentrate to the nameless company I work for. I will do my research as qualitative research.

Even though it is not very likely, there is a risk that someone would like to steal peoples or companies data from their meters and try to get some benefits with that information. There are also people that have access to that information. I will take a look at following steps of how the consumption data is delivered from a meter to the service provider

- Meter
- Possible ways how meter data is transferred to meter service provider
- Data Concentrator
- The metering service provider

- Electric utility

I will also take a look at the people who may have access to the data. There are several possibilities:

- Customer
- Anyone able to see the meter
- Installer if there are some problems with a meter or data transferring
- Employee of the meter service provider
- Employee of the electric company
- Anyone who is able and willing to brake in to electronic lines and willing to follow the PLC traffic, for example

According to Finnish bureau of information security, the main points in information security are:

- Availability
- Confidentiality
- Integrity

These mean that the information needs to be available easily for those who have rights to use it. Even though it is secured and behind the locked doors, intranet or just behind a password, the people working with the data needs to have access to it. *(Availability)*

With the *confidentiality* it is meant that only the people who have rights to use some information have access to it.

The *integrity* means that the user must be able to trust that the information is correct. It must be impossible or at least hard enough to change by accident or in an attack or at least it must be possible to confirm those changes and fix them.

After these three main points are often mentioned three other important points. They are:

- Non-repudiation
- Identification
- Authentication

Non-repudiation means that user cannot deny what he has done. There needs to be a stamp of every change made and of who has made it. It is very similar to one of the main points, the

integrity. This one points to the availability of showing the changes and confirming the person who has made them.

Identification. The user must always be possible to identify. It needs that the changes can be pointed to a username, even though the username can be anonymous.

Authentication means that the user is possible to authenticate as legal person. The authentication needs to be trustful. For example in the company systems the administrator must be able to identify the user, so in these cases the user cannot be anonymous. (Valtionhallinnon salauskäytäntöjen tietoturvaohje 2008)

Making something to be impossible to break is never possible. There are always ways to break in from some point. A company or a device has to be hard enough to break in to. It depends on few details how hard it must be. How important it is to keep the data confidential? How much would it cause losses if someone broke into the system? How much would the attacker get benefits of a successful attack? If someone was able to break in to some information, how long would that take and does the data still need to be secret after that supposed attack time? All those make a difference to the needed level of security. It is always needed to compare the costs of a successful attack and the potential losses of the attack. There is no reason to get that heavy and expensive security system that it costs more than the potential losses after the attack.

As background for this research I have used other researches about information security of smart metering, information security guide of Finnish government, Guide to analyze risks to improve information security of Finnish government and global news articles. I have also made two different interviews with different metering service providers in Finland to gather more information for my project. Because the object of my thesis is information security, both of the interviewed persons have not been willing to have their names published. I will not name the company that will be using my research either. Any specified information about the holes in the system and possibilities for a misuse will not be mentioned here in my thesis. They will be used by my employer to avoid such risks and to ensure reliable electricity metering for hundreds of thousands users in Finland.

There are some researches done before about the information security of smart metering. Pike Research has been publishing updated versions every few years. The newest of those, published 2010 has been used during this project. P. McDaniel and S. McLaughlin completed one 2009 and some others have been researching the security too. Still there have not been many investigations about the smart meter security yet. And most of those researches that have been done are very hard to find unless you have connections to the metering companies.

As the meters come more common across the world during the next years, I suppose they will be investigated more.

2 Smart metering in general

Electric companies worldwide are installing new so called smart meters to follow their customers' consumption. Those new meters have lots of advantages the old ones did not. It is possible to read the meters remotely and the utilities may have the consumption data daily, even hourly. With the new meters utilities don't even need to send an installer there to disconnect or connect the meter or change its tariff. Also in the countries where people use more gas at their homes, for example by using gas ovens for cooking, it is possible to have the same meter to follow electricity and gas consumption.

Smart meters also give electric utilities possibility to have new services to customers. People will have possibility to minimalize their consumption when they can follow their consumption hourly based. Utilities will be also able to run demand response programs, where customer will not need to do anything in order to get a more efficient energy use, from both utility and end-user perspectives. A good example of this is the night electricity, which makes it cheaper to use for customers and decreases the load on the grid so it's also good for the utility.

Finnish government wants that at least 80% of electricity meters are changed to smart meters before the end of the year 2013. In fact, that milestone will be handled much earlier. For example E.ON has completed it in 2008 and Fortum has already installed most of its 600 000 planned meter installations in the late 2013.

The state started to pay some money for utilities from all the installed smart meters that are sending consumption data hourly based before the end of year 2012.

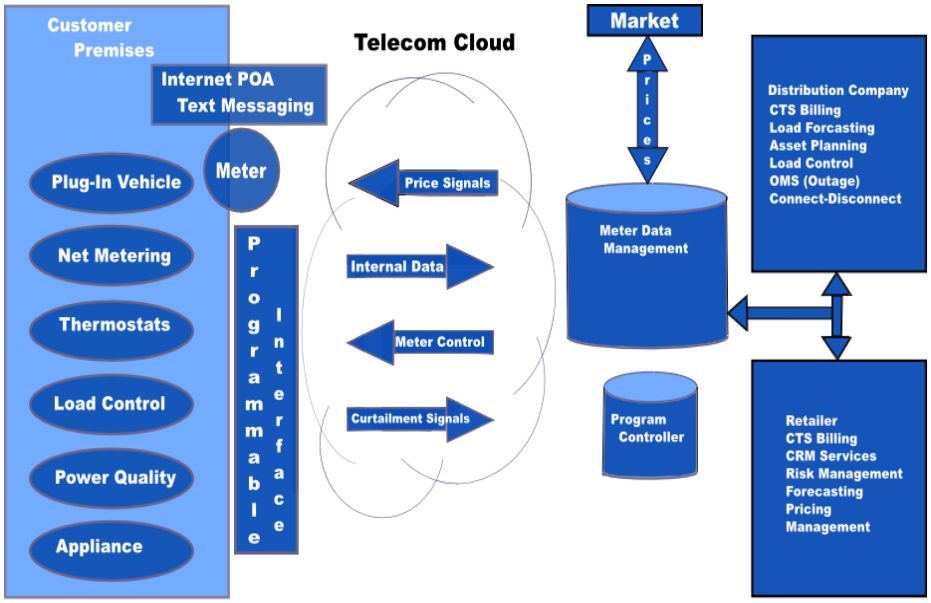

Figure 2: Data flow in smart meters

2.1 Meters remote reading

In this chapter I will take a look at different ways smart meters communicate with the utilities system. There are few different ways how the meters send their data to the electric utility. I will have more specified information about those meter types used also in Europe and will mostly skip those used in the US.

2.1.1 Point to point meters or 2p2

There are several ways how the meter sends its readings to the utility. One way is point to point meters. In that case there is a sim card in every meter and it sends the reading in mobile network. That is used mostly in areas where there is a long distance between the delivery sites and therefore to other meters or where there are some devices that causes some continuing disturbance for meter reading. Also it is common for places where the consumption is large, for example in factories. They have some advantages like pretty confident communication to the meter reading systems at least in Finland, where almost the whole country is under mobile network coverage. Still, it is pretty expensive to have every meter communicating by themselves.

2.1.2 PLC network

Some service providers use Power Line Communication (PLC) network to have the readings. In those cases, there are several meters and a data concentrator (or DC) around the same transformer. The meters send the consumption data to the DC via power lines. The DC has connection to the mobile network and it sends the data to the service provider.

The DC can be installed to the transformer itself or to some customers' properties. The most effective way is to have it installed as near the center of the transformer as possible. Then the meters will be able to send the data straight to it and will not need any repeaters between them. In such a case it is also the most trustful that the data deliverance works all the time. The best solution is still to install it on a transformer or a house that has always electricity turned on. If a concentrator is installed on a delivery site where it is, for example, some ones summer cottage, there may come problems to the data reliability. Often when people leave their summer cottage, they do switch off their main switch and that turns also the DC off. In such a case none of the meters under the same data concentrator are able to send the readings as long as the DC has no electricity. Because of that, some meter service providers install the meter before the main switch and therefore the meter or the data concentrator sends the data even though the main switch is turned off.

2.1.3 Radio signals or radio frequency

Radio signals are also one possibility for transferring meter data from a meter to a data concentrator. The meters are installed in the same space. They all are wired and connected to a radio signal transmitter which sends the data to the data concentrator.

There is already some Radio frequency -mesh systems available in the market. Each meter is equipped with a radio transceiver, no need to wire several meters to one signal transmitter.

Any Finnish meter provider does not use this way. The use of RF-mesh in Europe is very limited because of the network topology. Highly populated areas in urban scenarios and rural networks are not very convenient for RF-mesh. Radio frequency signals can be disrupted with the same difficulty than PLC and there is no difference in terms of security.

2.1.4 Data concentrators

In all smart metering systems the meter sends the data it is holding to a data concentrator except the point to point metering system. Also the commands from the maintainer are sent

through the DC, which will route the command, for example a remote disconnection command, to the meter.

The concentrator gathers the information about consumption and meter errors et cetera and delivers the data to its service providers system. Data concentrators are installed in some cases to people's delivery sites behind the meter but the most common way is to install them to a transformer. Mainly the DCs are installed on delivery sites at countryside where there are not so many meters in a larger area and there are only few meters under the concentrator. In the towns the DCs are usually installed on transformers and might have at maximum 1 000 meters under them.

Having information up to 1 000 meters and their consumption data up to one month and the data packages are larger, so it is important to have the concentrators communicate reliable with the service provider. DCs communicate in usually mobile network, which is reliable, well protected network and usable in whole Finland. Still it is possible for DCs to use any other Wide Area Network technology to connect the DCs with central systems. Virtually a DC can be connected to any available WAN technology.

3 Potential technical issues and issues with meter working environment

I will have a look at the possible issues according to smart metering systems and the people who have access to the data the meters hold. I will start with issues of personal use and use in business environment. Later I will take a look at the technical issues and the issues caused by people who have access to the meters or the data they are holding.

I will have a look at the possible technical issues of the meters and how the information is sent from meter and delivered to the electric utility. I will have a look at every step where the data goes and think how it could be delivered more secured.

Smart meters must be viewed in both contexts, as part of the entire grid and also part of home area networks. If parts of a network are individually secured, it does not make it secured network. Smart meters have to be secured in a way that the meter or its data cannot be used to attack the other devices of the network or the grid itself. (Lockhart, Wheelock 2010, 8)

Smart meters may be parts of two networks, a home area network (HAN) and smart grid. So in theory smart meters might bridge the HAN and the grid, which can be counted as a neighborhood area network (NAN). These two networks are mutually untrusted, so they must remain separated.

There are several services that let utility to build and run a more secure smart meter network. (Lockhart, Wheelock 2010,12)

3.1 Issues with personal use

There are not many reasons for anyone to attack electricity meter of his own or anyone else. While the main thing of the meters is delivering consumption data from a customer to his electric company for invoicing data, there are some other functions as well.

With correct information a potential customer could connect the meter allowing him to use electricity without having a contract and therefore without paying. The same thing would be possible for a customer who has not paid his bills and whose smart meter has been disconnected. It could also be possible for customer to distort the consumption data to reduce his bills. In these possibilities the utility would lose some money. The sums would be pretty small compared to electric utilities cash flow but still it would be loss.

Most likely no one would be hacking just one meter to gain small benefit for himself. If a hacker would be able and willing to hack a meter, most likely he would try a massive strike attacking at least thousands of meters.

Smart meters gather much information about its user. Gathering that information could give the data holder information about the consumers' way of living, potential diseases, devices he uses at his home and even times when he's sleeping. That is a reason why European Data Protection Supervisor (EDPS) finds a lot of privacy issues in smart metering. (BBC news 2012)

Also, by following people's consumption data some burglars could see when the residence is empty. That would allow them to rob the house without anyone noticing it in a long time. The same information can be seen more easily by going to the house itself. By going to field to check it, there is much bigger risk to have someone eye witnessing the investigations. By checking the information from the screen, it's harder to find out who has been investigating it.

3.2 Issues in business environment

An entrepreneur could disturb rival companies business and stop their production by shutting down their factories electricity entry. That could cause the loss of millions of euros in a day in, for example, paper industry, where it takes days to get the machines turned on again.

Even a tariff change of a factory could cost enormous amounts of money before it was noticed in the company.

Therefore it is very important to have all the meter communication secured. All the connection and disconnection commands need to have a correct password or a key and the meter needs to send error messages to the service provider every time someone makes configurations to a meter.

3.3 Privacy issues

Data privacy is one of the most important issues in security. Every country has detailed laws to protect consumers' information. Breaking those rules lead to some kind of a penalty, in some cases even criminal liability.

Smart meters, especially when connected to home networks, capture a lot of personally identifiable information. Such information is a subject of data privacy legislation.

Many benefits of smart metering can only be found by capturing personally identifiable information and analyzing it. So that information must be collected and retained and analyzed but the collector has to secure and protect the information.

When data is sent from home area network, it must first be decrypted off the HAN securing and then encrypted to smart meter networking format. Security mechanisms for HAN based on Smart Energy profile are really very strict. These are the HAN networks controlled by the utility. However there can be a gateway with the possibility to bridge Smart Energy networks with home automation networks that are controlled by customer, the gateway is a high risk in terms of security. Attacking the data packet during this, it makes the data vulnerable and opens a possibility to listen to the data. (Lockhart, Wheelock 2010,12)

Smart grids ability to manage load control makes it also possible to identify some specific devices in customers' homes or companies' offices. When this kind of information is used wrong, it allows burglars to attack searching for some special targets.

By following the consumption data, it can also be seen if the consumption reduces for some time. That may show the burglars that the customer is, for example, on holidays and there is no one home, allowing them to rob the house in private.

3.4 Risks about networks

It is not a valid security action to have a smart meter with possibility to bridge two networks that don't trust each other, the home area network and the neighborhood area network. That kind of solutions should be avoided and taken care some other way. Both, the HAN and the NAN, service providers consider their responsibility filled when they reach the meter.

Using the current technology, there are functional limitations in truly separating the networks. However, it may change when the meters gain more power. One solution could be an architecture that brings together home area network and the grid. Or maybe the solution might be some security procedure that can handle both of the networks. Despite that how it will be taken care of, until that the meter remain as the most vulnerable part of the grid. Only it carries the customer and utility data in unencrypted form. (Lockhart, Wheelock 2010,12)

When connected to grid, the meters authenticate to the manufacturers main system, such as Itron's OpenWay or Echelon's NES. Utilities must have process to make sure no unauthorized meters connect to the network. Also device deployment needs to be controlled. In this point, it is the most easy to follow procedures of Information Technology Infrastructure Library (ITIL). It provides good guidelines for change management and configuration management.

3.5 Meters

Smart meters are to be considered as network endpoints. Even though they have far less computing power than usual network endpoints, like computer or tablet, they are still potential targets for attacks. When creating a secure smart grid, smart meters need to be secure and also help other components of the grid.

At the moment there it is really hard to get unauthorized code added to a smart meter. There are two main reasons for that. First of all, the meters have so little computing power. Also, the meters operational systems are not well known. The operational system is developed for a specific use and there's not much space in devices memory for alternative builds. However, some manufacturers have begun to produce meter with larger code space and 32-bit processors. (Lockhart, Wheelock 2010,12)

Tools created for PCs, such like antivirus tools, are not practical for use on smart meter because of their size. They also need too much computing power. Tools like whitelisting exist, allowing only a fixed set of programs running on a meter. That may be the most efficient application to have meters secured at the moment. With whitelisting it is possible to do al-

most the same things as antivirus programs but with much less computing power. There are also operation system level change control systems that prevent any unsuspected changes in operation system. However, it is only possible to run these systems in meters that have more powerful operation systems, like Windows CE or different Linux variants.

To avoid large amount of administration for the smart meter service provider, it is important that the meters manage themselves as much as possible. For that reason it is unlikely that there will be any antivirus programs in the meters. It is also possible to control the operation systems changes from by meters administration tools. So the meter service provider is alerted if there comes some unexpected changes to meters system.

However, cheating a meter is possible. The meter authenticates itself to the utilities central system via private key. Only that public key of a meter will successfully decrypt transmission the meter, which allows it to identify itself. But the chip holding the private key might be removed or moved to another meter. There are several different private keys present on the communication chip. Each of those is for different function but all of those have the same risks. (The Guardian, 2013)

To try a cheating attack for a meter, the attacker needs to have and use the meters private key. Most easily it could be done by removing it from a meter that has activated its private key. There are several other ways to get the keys. For example, some employee of manufacturing facility could spread a list of smart meter private keys if the person gained something by doing it.

As long as the meter authentication occurs via communication chip, utility may never suppose that there happens no cheating. Instead the utilities should accept that there is spoofing and the meters will be compromised and work to minimize the damage it will cause. A corrupted meter should not have possibility to cause damage to other devices in the grid.

From the internet can be found stories where the meter has been taken away from the smart grid and hacked. It must be remembered that the hackers have not had possibility to try the device in the environment where they are meant to work. They may not have tried the meter software in its functional environment either. So the information they have got is not totally trustworthy but the information they have found should be understood and pointed when planning security architecture for smart meter grid.

Some meter types, mainly the ones used in the States, have also been possible to hack to manipulate its results. According to FBI, it has already caused the loss of hundreds of millions of dollars. It has been easy to manipulate the results with free software found from the inter-

net and optical connection how to connect the meter to another device, for example PC (Krebs on Security). With the meters used in Finland, the results are collected daily including hourly values and it causes an error to meter information log if the result decrease. So the meter should be manipulated not to collect all the consumption. The models used in Finland are more secured and would send an alert to service provider if tried to be hacked.

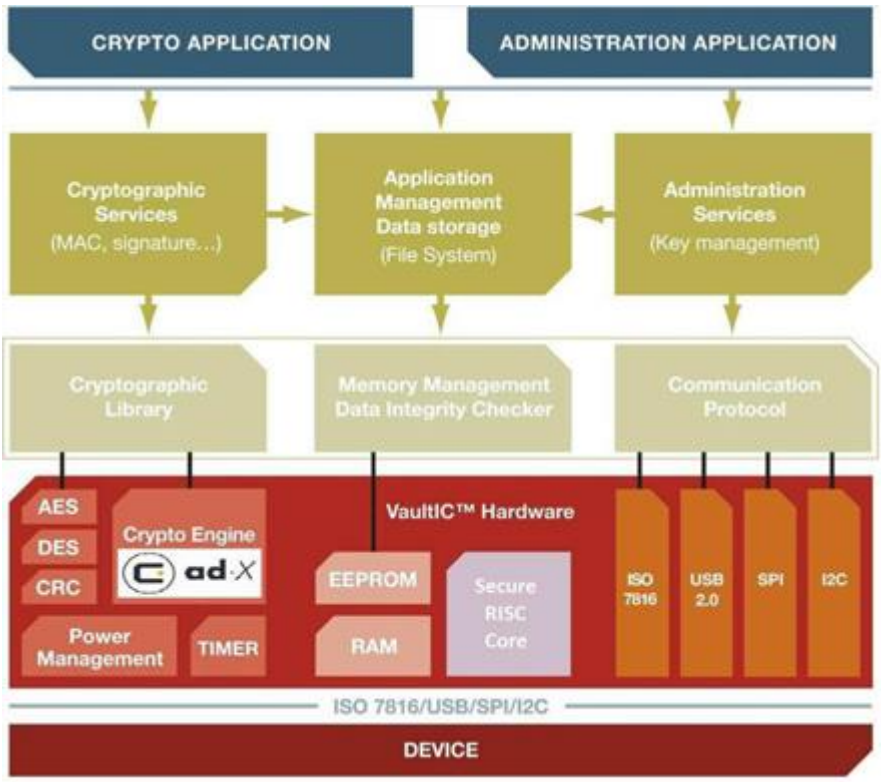

Figure 3: Meters security management

3.6 Data concentrator

The data concentrators are usually installed in places where they have the best possibility to communicate with the meter. Because of that, they are also in places where it is most easy to eavesdrop their data signals. However, the installation places are usually public and easy to see. Many of the DCs are installed on utilities pole. In my point of view, it is more assumable that a potential hacker tries to attack a meter in the quiet backyard of a customer than DC in pole in visible place.

So the highest risks in data concentrators are eavesdropping and that someone tries to block its communication to the meters or the utility. Utilities have to have procedures that make it as hard as possible to anyone to deny the communication. The meters must not, for example, lose their functionality if they have not a working connection to the utility or concentrator. The best for the utility is if they can even save the consumption data from few days and send

it when the meter or the DC has its communication working again. It is also the usual way the data concentrators work.

Listening to the data sent in PLC network or to RF relay is pretty easy. PLC network is created for delivering electricity to the customer, not for intelligent network. Main purpose for radio frequency is mass informing. So in neither of the cases, there is no way to secure the data from eavesdropping they are transporting. If someone is willing to have, for example, PLC modem, he is capable to listen everything that happens around him. As mentioned before, all the data coming from the meter must remain encrypted as long as it takes to reach the utilities central system.

Manipulating the concentrators' data is, as in meters, hard. The concentrator works pretty much the same way as a meter. There is an operating system that is built for only the specific use and there is not much extra memory in the device. To have a possibility to change any code there is in the concentrator, the hacker should have the public keys. So when the meter sends consumption data to a data concentrator, the data received from the DC is pretty trustworthy.

DCs use mobile network to send the data they're having to the metering service provider. It can be considered as one of the weakest point in meters communication chain. Access to the WAN service provider' infrastructure is be on the door of central systems. Main barriers for hackers have to be placed here at this point.

3.7 Metering service providers database

The metering service provider needs to save the consumption history to its databases for, for example, invoicing purposes. As every company, the service provider needs to take care of its systems security. It needs to be taken care that no one can access their customer information or any confidential data. The systems need to be well secured and behind good passwords that are changed often enough. If the information can be checked only from some particular network and needs a VPN connection if checked outside the normal route, specific programs and applications with good passwords and backtrack for things that are done to the meters, that can be considered as secured way.

For optimal security state all the potential issues in service provider system and network need to be quickly fixed and there also need to be backups for all the potential data about the meter or data concentrator or, for example, the sites where they are installed or the consumption.

3.8 The electric utility

Just like other companies, for example the metering service provider, also the electric utility needs to take care of it information security. The systems have to be secured with virus protection software, firewall and good unpredictable passwords. The company must have its customer information in secured database with access control denying unauthorized users from seeing or modifying the data. There must also be backups from both, the data about customers and the systems. If company gets attacked or their databases crushed, the information needs to be available for returning.

4 Potential issues with people accessing the data

In this chapter we will go through the persons having access to the information and the treats that will cause.

As always, the greatest danger to information security is the human handling the data. If an employer of any company looks at any information that he does not need for accomplishing his work, they should be properly punished if breaking the targets privacy. This means all, no matter if it is, for example, a nurse checking the medical history of some relative or celebrity, police checking his son-in-laws criminal records or electric utilities employer looking at his neighbors' consumption.

4.1 Customer

The customer is the one who might have the most interest to manipulate the meter data. He might be willing to reduce his bills by reducing the information the meter sends to the electric utility. As we noticed earlier, getting some device to interrupt the meter from sending the data does not help to avoid getting the invoices.

In about half of the cases, the customer has access to his electricity meter. In those cases he's always able to see the data from the meter. Some people might also be trying to bypass the meter by themselves and steal the electricity. Once in a while there are such cases in Finland. Usually they are noticed in some months and they will face consequences like compensation.

The customer might also try to cause some problems to his meter to have the electricity company bypass it. When the meter is bypassed, the customer uses legally free electricity. That is why the utility has to keep track of all the field visits they make and be sure they fix

the possible bypasses in short time. Having it forgotten, the customer might be able to use the electricity free for even several months.

In some cases, the customer might also be willing to hack the meter. You can connect you PC or some PDA devices with cable to a meter. Doing that would endanger the reliability of the information. As noted before, at present adding some unauthorized operating system to a meter or upgrading it would be difficult because the meters have so little computing power and they use operating system built for specific use.

Customer could also be willing to connect his meter without having contract with the utility. That would allow him to use illegal free electricity, just the same way as customer reconnecting the meter utility has disconnected.

The meters have to have an authentication key to deny customers from doing that. Some companies doing the smart metering in Europe have a unique key that is sent to installer every time when there is some need for configuring or connecting meter. That is quite hard to break and therefore a good proof of customers not having possibility to reconfigure the meter. For example I would mention at this point a couple of alarms at the meter level that helps to identify whenever the customer is trying to do a fraud. Meter cover alarm is sent to central system if someone is opening the cover. There are also some other alarms which can infer an intentional fraud. Also the meters usually have magnetic tampering alarms when a magnet is located nearby with the purpose to affect to the measurement circuit.

Utilities need to have some way also to interfere customers from bypassing the meters.

4.2 People with possibility to see the meter

In cases where the meter is installed at the customer premises, there are two options for the installation place. It is installed in customer house or, for example, at the wall of some building of the customer.

Having it installed inside the house, the people might see it when visiting customer but there is not much use for the meters data. What would someone do with the consumption data? I cannot imagine a thing. It is a risk for customers' privacy but the information will give the visitor no advantage.

When the meter is installed outside the house, a potential burglar can see that the building is not in active use. Following the consumption will let the burglar to see when it is safe to go and rob the building. Still, there is no need for the potential attacker to see the meter. One

can see it before reaching the meter if the building is not used. There are neither foot prints in the snow nor there are laundry getting dried on the field or a car in the parking slot. Just a visit to the yard gives all that information for planning the attack. It would be a different thing someone had ways to follow that information from the web. To that we will take a look at chapter about metering service provider.

There are not much risks of having the meter seen locally. That information is for no use to almost anyone and the ones that could use it will have the same information by following the happenings of the site for just a moment.

4.3 Installer

In a point when some metering service provider is installing meters to some area, the work is done pretty quickly. The main goal is to install as many meters as possible and after that make sure that the meters just installed are working. In the metering projects, the utility wants that at least some percentages of the meters are communicating with the service providers systems. There are always some earlier made plans of the percentage but every area is different so they will be checked one by one. Every area has its own detailed contract. For example, if the installations are going on at winter time and at the area there are lots of summer cottages, there will be lots of places where the installation is not possible. In those cases, the missing installations will be done later when the installers have access to the property. On the other hand, in towns or cities most of the buildings are apartment buildings and the installers have access to them anytime they need. In such a case there wanted percentage is way larger. Let's say that in average, the sum of communicating meters has to be about 95 percentages.

When the metering project is going on, the installers are installing the meters in hurry and there always comes installation errors in some of the meters. Installing a meter so that it does not collect all the consumption is possible. Still, it would require such a bypass it would not be just counted as an installation error when noticed later.

If an installer would be installing a meter to place of a friend or relative of his, it could be tempting not to gather all the consumption. It would be a motive to give some benefits to a friend. In these cases there are certain alarms at the meter level and also quality checks at the utility that can raise the suspicions of a fraud.

As noticed, it is important to have follow-up for also the people installing the meters. Every step needs to be followed and confirmed that they do their work properly. But by doing installation errors, the biggest problem is not causing some minor losses for an electric utility.

It might raise a risk of people having fires, water damages or broken electrical devices at their houses causing large reparation costs for the company installing the meter or for the utility in charge of the installing progress. Fires could also cause deaths to people living in the apartment or a house.

After the installation is made, there are some cases where the installer has to visit the site again. There might be some problems in the meter or, as we noticed earlier, suspected electricity stealing cases. The meter might have problems with sending the data to its data concentrator or the service provider might need to send an installer to check the possible errors if the meter sends no data to their system. When someone makes a new contract to the electric utility or ends his contract, a smart meter is either connected or disconnected depending on the customers' situation. With smart meters, it is possible to do both of these things from the service providers' office remotely. Still, if there is even a minor disturbance in a PLC network or the DC cannot communicate, the remote connection fails. The same problem comes even if the customer has switched off his main switch and therefore not letting the meter to get electricity. In the cases mentioned, the service electric utility will need an electrician to visit the meter and check its functionality. Because of that, some companies installing smart meters use a way to install the meter before the main switch and that way make sure the meter gets electricity even if a customer turns off his main switch.

The installer has an access to the data stored to the meter and he has also the skills and equipment to read, connect, disconnect or reconfigure the meters firmware. So there are lots of things the installer could do if he had some motivation to make the fixes. There might not be many advantages for the installer to do any unauthorized changes but a customer might be willing to, for example, pay him of reducing the data meter sends. Naturally, most of the installers would inform his superior about such suggestions. Not doing so would risk his work. Also the firmware and configuration changes would be seeable from the electric utilities and metering service providers systems. It is very important that the metering service provider not only is able to follow all the configuration changes made to a meter but also doing that follow-up. Trying to reduce that risk when an installer visit is needed, the installer will have incident with some specific service type which allows him to do some things but denies others. Usually they have right to read the data but may not modify anything.

4.4 Employers of a smart meter company or electric utility

Rights to read data on customer power consumption must be given only to the people who need them to do their work. For example no ICT staff should have access to any production data. Still, there are always situations where there are some problems with any kind of system and ICT staff needs rights to fix them. For such cases there has to be some root ID. The

use for that root ID should be done as secured and easy to follow as possible. For example, some software that creates log of every time it's used and creates a new expendable password after every use. There are some commercial software's for such a use.

An employee of a smart meter service provider or the utility who has access to the customer data might be a risk. As noted before, with such information it is possible to know when the customer is not home. With such information an attacker could know when it is a potential time for emptying the house from everything valuable. The employee can also collect information that violates privacy laws about customers.

In the media have been some scare stories about possibility to mass disconnection of services when utility is using smart meters. At the latest, Finnish Broadcasting Company published news about meter hacking saying that "a hacker could disconnect all the electricity from a town" (YLE). Based on the Smart meter security report from Pike Research, this kind of attack would be hard to execute even as inside job (Lockhart, Wheelock 2010,17). Such command would need authentication from a meter and central system. Only the sender could have the correct private key and therefore successful decryption authenticates the true sender. If the command succeeded, the one would be easy to identify and had no possibility to claim someone else did the command.

Also, the commands to meter have very short time to live. If it takes too long to get the command to the meter the meter would think the command was too old and time out. If tried to send that kind of a command to all the meters via PLC, the grid would have so much load on it that it most likely would time out most of the commands.

Still, there are some technologies which allow massive disconnections with broadcast commands to reduce consumption peaks, so that kind of an attack would be possible to accomplish.

Think about a situation where an employee of the meter service provider hears that the company is going to denounce some of its employees. He believes that he will be one of those to be dismissed and starts planning retribution. He might be in a position where he has access to the meters and skills to operate them. If he has skills to operate the meters, he most likely also knows how to do damage with them.

Most of the employees handle it well if they are to be separated from a company. However, in all cases it must be ensured that an employee may not have possibility to revenge even if he wants to. Employees should have no access to any critical systems after they know they will be separated from the company. On the other hand, it would not be a good way to tell

that to the employee by letting him notice his logon IDs are no longer active. So a good way to handle such things is active ID management that inactivates IDs when that is needed to be done. Also the maintenance programs should deny the possibility to do any grater harm for the meters or the system. Password policy for people leaving the company is really important. (Lockhart, Wheelock 2010,27)

5 Risk analyzis

In this chapter I will make analyzes for few risks. According to Finnish Ministry of finance, when managing risks, company should take in consideration the seriousness and the likelihood of the potential consequences. It is important to figure out the largest risks, which need to be solved instantly. (Ohje riskien arvioinnista tietoturvallisuuden edistämiseksi valtionhallinnossa, 2003, 41)

5.1 System attack

As mentioned above, it is important that the companies holding classified information have their own systems secured. The company that will be using this research to improve its information security has its main systems pretty well secured. Accessing to their systems needs that the user is trying to connect from the right IP address and have correct passwords. Still, there are thousands of data concentrators around Finland and all of them include a chip which allows tunneled connection. The tunneling has at the moment some faults in its configuration and therefore it allows connection to even those systems it should not.

So it is possible to achieve the risk for those who have access to those chip cards. Still, most likely there will not be much interest for such attack. From the likelihood I give the company 1 point (scale 0-3).

If someone accomplishes this risk and gets in to the companies system, it has immediate influences. It affects on all of the users and all the systems need at least days of downtime to have all the systems reconfigured. It also compromises the classified customer information of all the customers. Such a threat should also be informed to the media and ministry. In the worst case, where the attacker will be mass disconnecting the electricity from tens of thousands of people, it will cost large losses when happening. So about seriousness I give the risk 3 points (scale 1-3).

So the risk got 4 points out of 6. According to Finnish ministry of finance that 4 out of 6 points means moderate risk. It is not critical but needs to be taken care. (Ohje riskien arvioinnista tietoturvallisuuden edistämiseksi valtionhallinnossa, 2003, 41-43)

I have informed the company about this risk and it will be taken care that the tunneling will be reconfigured. In the near future that tunneled connection will open access only to the systems that the devices need.

5.2 Hacking multiple meters

If someone is willing to hack multiple meters, he needs to first be able to attack the companies systems. As mentioned before, it is possible still for some time until the fixations. After that he needs to be able to feed the corrupted code to the meters. It is very unlikely that someone is able to break in to the systems to hack few meters. It is pretty well secured and should be noticed almost immediately. So in my point of view, this risk gets 1 point of 3 in likelihood.

If someone would attack the systems and manipulate multiple meters, it would cause extra work for at least one expert until the problem got fixed. It also has effect on multiple customers. Still, the problem would not cause large amount of financial losses. All the other meters could be kept in work, only the manipulated should be fixed and even though all the systems should be taken down, changing to companies alternative (failure) server cluster it would be possible to keep the systems up all the time. So from this risk I give 2 points out of 3 in seriousness.

So this risk gets 3 points out of 6. According to Finnish ministry of finance that 3 out of 6 points means minor risk. It needs to be followed and made sure that the risk is under control. It doesn't need any immediate actions but it should be considered if there is a more secure way to accomplish. As mentioned before, the access to the systems with the chip will be reconfigured to be more secure. Risk for this kind of action will reduce at the same time. (Ohje riskien arvioinnista tietoturvallisuuden edistämiseksi valtionhallinnossa, 2003, 41-45)

5.3 Manipulating one or few meters

If someone is willing to manipulate one meter, he should get the meters private key and have access to the meter with his computer or PDA. As all the meter private keys are hold by metering service provider or the meter supplier, getting that key would need a successful attack to the smart meter company or help from the company. It is also very unlikely that anyone would want to manipulate only one or few meters. There would be no benefit of it and if hacker would be capable of doing that, he would most likely try something bigger. So from this scenario, I would give 0 points out of three in likelihood.

Succeeding in such attack would not risk the data of anyone else. It would not either cause immediate actions. The worst case would be that customer would be getting free electricity until the utility notices the manipulation and the costs would be only hundreds of euros in maximum. It would not cause downtime to the systems. So from seriousness I would give 1 point.

So this risk gets 1 point out of 6. According to Finnish ministry of finance that 1 out of 6 points means minor risk. The risk is so small there are no actions needed. (Ohje riskien arvioinnista tietoturvallisuuden edistämiseksi valtionhallinnossa, 2003, 41-45)

6 Steps to improve security

The companies maintaining the meters use different kinds of softwares to operate the meters. For example one of the companies I have been communicating to about the meter security uses the meter manufacturers' software to some maintaining issues and systems of their own to others. Many of those systems never ask to change password and some are even running with the default passwords. That company should take some new policies to manage their security issues. They should make changes to their software configurations and start forcing users to change their passwords at least every third month.

It would also be good for the companies security to use SSL to secure users logons in their own web applications. That would make it more secured to logon to the system and the data the systems hold would be easily made more confidential.

Logins from any non-personal id must be denied. As far as I know, that is done with most of the systems. Still it is possible to log in for example to the meter manufacturers softwares with a general username and default password. Such a behavior should never be possible and I have communicated to the company about the need to reset passwords and denying the non-personal username.

I have also gained such information that if a hacker gets tunneled connection to the meter service provider, for example by stealing a chip card from a data concentrator, the tunneling is made with such configurations that the attacker would be able to access to any server of the company. That should be changed immediately so that from connection of those chip cards it is possible to access only to the servers that the connections need.

I think also the systems and protocols that use plaintext should be replaced with secured alternatives.

7 Summary

As noticed before, there are some threats in smart metering. The risks are pretty small and will be able to avoid by having information and the systems of the companies maintaining the meters secured well. The companies maintaining the meters also need to be very accurate with who they hire to the tasks where people handle classified or confidential data.

Most of the risks are about the people's privacy as the service providers are able to follow so well about the consumption data. There is also a risk that someone will be trying an act of terror with the help of smart grid and is able to shut down a whole county.

A good way to avoid the risk of following people's use of some specified devices is that the metering company does not have customer data. They only have data of the delivery site and will get information of the customer only when a field visit is needed and they will not be saved to the metering companies databases.

The meters are hard to hack and possible tries will be noticed pretty soon. Their system does not have much space to change the way they work. Also the corruption of meter results is a small threat as the meter always sends a notification of every single change made to the main system. No one can even open the locker of the meter without the notification sent to the central system.

Also, trying to hack one or a few meters does not sound reasonable. What would make any sense is to make a massive hacking for at least thousands or tens of thousands meters of some company. In such a case the hacker would gain access to hundreds of thousands peoples consumption information and would be capable of following when people are not at their homes or summer cottages or would be able to disconnect electricity from, for example, from a whole town. Alas, that would need a successful break into the meter service providers systems. As every company, the service provider and the electric utility has to count what does it mean for them if some unauthorized people get the data they are holding, how long that data is valuable for those unauthorized people and what can they do with it. They have to count that how secured system is reasonable for securing the data and how much they are willing to pay for keeping that information private.

In the companies I have been in touch with during this project, I have seen that the Finnish utilities and metering service providers have their systems secured many ways. The data going from a meter to the utility is always encrypted, the systems and antivirus software's are being kept up to date and the meters communicate with the service providers many times a day and if they are not, the service provider will find out the reason why they are not com-

municating regularly. Still, there are holes in the way to connect to the main systems that need to be fixed. Tunneled connection with a stolen chip card allows the attacker to do too many things to the systems. Even disconnect the electricity from hundreds of thousands of people.

Like in most of the cases, the largest security risk is the employer of the utility of meter service provider. They have the access to the data, they know how to read the information and no one would be surprised about following and researching the data. They also have tools to configure the systems. So, utilities and metering companies should be very secure about what kind of people they are hiring. They also need to make sure that people who are being separated from the company will have no possibility to avenge it if they feel they have not been threated right. For example, if a person operating the meters is being fired, company has to be sure that the person may not be following the consumption data of its customers and may not be able to disconnect all the meters. The operation mentioned at the latest would cause massive problems if it succeeded. It would cause the utility and the service provider to lose their electricity. If the service providers systems would be disconnected and run out of electricity, getting the systems up and working again would be very complex. And before they would work again, at worst hundreds of thousands apartments would be out of electricity. If someone succeeded in that kind of terrorism, it would cause losses of at least hundreds of thousands euros to the utility. The service provider has to be sure that no such issues will happen and also that no one is able to attack to its systems so that he would be able to disconnect the meters.

What is also important is to be able to track every single change made to the systems or meters. The service provider has to have possibility to name the person who has done any changes to the systems or the meters. That makes the system more open and therefore people working with the systems and having some thoughts of harming the company might think that they will be caught for sure and it will cause some consequences. That most likely makes dissatisfied employee to think another time and decide not to do such harmful act.

Also, as the system is as open as possible and the administrators can trace all the improvements made to it, it helps to find the reasons for errors that, for sure, once in a while come out. An error might appear, for example, after upgrading any part of the system and they may not be found out right away. They might in some cases be noticed way later when some another upgrade for another software or application is no longer compatible with the upgraded version and that causes crashes. It even isn't the worst situation if it causes a crash. The system might also tell that the failing command has been successfully executed and the fact that it has not will come out in some follow up or while investigating some other issue. In

such cases, it may be the easiest way to find out the source of the problem if the system administrator tracks down the changes that might cause the incompatibility to those softwares.

8 Self-assessment

During this researching process I have found difficulties in finding enough material about information security on smart metering. And those researches I have found have been few years old, which is pretty much in business that is developing really fast. That has made some difficulties in my writing process.
I have also found some issues in my own writing process. I should be more logical when creating the headings. I would also need more logical order to make it easier to read for a potential reader.

Regardless of these minor issues that I could improve, I find this research quite well accomplished. I have lots of information about the subject and even though the subject touches most of the Finnish people, there are not many people knowing enough about it. The basic information of the smart meters is found from my research but there is also a lot of specify information for those interested of the information security. The research will also be used to ensure that several hundreds of thousand meters of one company will be secured better.

I also could have been more intensive while during this process. Even though I did it while being eight hours a day working, I still would have had possibilities to accomplish it months ago.

List of References

BBC news (http://www.bbc.co.uk/news/technology-18407340 , the article was read 17th of February 2013).

Gray, G. R., *AMI Enterprise, A Framework for Standard Interface Development*.

The Guardian (http://www.theguardian.com/technology/2013/aug/18/smart-meters-uk-hacking-electricity , the article was read 3.10.2013).

Krebson Security (http://krebsonsecurity.com/2012/04/fbi-smart-meter-hacks-likely-to-spread/ , the article was read 17th of February 2013).

Lockhart, B. & Wheelock, C. Smart meter security, Pike Research.

Ohje riskien arvioinnista tietoturvallisuuden edistämiseksi valtionhallinnossa.

Valtionhallinnon salauskäytäntöjen tietoturvaohje.

Yleisradio (http://yle.fi/uutiset/etaluettavissa_sahkomittareissa_tietoturva-_ja_yksityisyysongelmia/6525339 11.03.2013, the article was read 12th of March 2013).

Table of Figures